To enhance mission performance, TSA is committed to promoting a culture founded on its values of Integrity, Innovation and Team Spirit.

1. **PURPOSE:** This directive provides TSA policy and procedures for properly managing software applications, to ensure compliance with Federal regulations and copyright law, and to aid in the overall support and maintenance of all TSA information technology (IT) resources on the TSA Enterprise.

2. **SCOPE:** This directive applies to all users of TSA's IT software resources including full-time, temporary, and part-time employees, volunteers and temporarily assigned employees, and contractors providing full-time and incidental support.

3. **AUTHORITIES:**

   A. 48 C.F.R. Part 39 Federal Acquisition Regulations , "Acquisition of Information Technology"

   B. Aviation & Transportation Security Act of 2001, 49 U.S.C. § 114

   C. Clinger-Cohen Act of 1996, 40 U.S.C. § 1401

   D. DHS Financial Management Policy Number 003, Accounting for Internal Use Software

   E. Executive Order 13103, Computer Software Piracy (September 30, 1998)

   F. DHS MD 0007.1, *Information Technology Integration and Management*

   G. DHS MD 1120, *Capitalization and Inventory of Personal Property*

   H. DHS MD 4900, *Individual Use and Operation of DHS Information Systems/Computers*

   I. TSA MD 1400.3, *TSA Information Security Policy*

   J. Office of Management and Budget (OMB), Security of Federal Automated Information Systems Circular A-130, Appendix III

   K. Procurement Integrity Act, 41 U.S.C. § 423

   L. The Accounting and Auditing Act of 1950 (31 U.S.C. § 65)

   M. The Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030

   N. The Computer Security Act of 1987 (P.L. 100-235), 15 U.S.C. § 278

   O. The Federal Managers' Financial Integrity Act, 31 U.S.C. § 6103

   P. The Privacy Act, 5 U.S.C. § 552a

Q. U.S. Copyright Law, 17 U.S.C. § 105

4. DEFINITIONS:

A. Applications Software: A classification of computer software programs designed for a specific purpose (such as accounts receivable, billing, or inventory control) or to satisfy a set of user requirements.

B. Approved-client Application List: A list of Client Applications that are listed on the DHS Technical Reference Model (TRM) for TSA's use and have been tested in the COTS lab and maintained in one list.

C. Commercial Off-the-Shelf (COTS): Any item other than real property (e.g., software, hardware, or computer product) that is ready-made and available for sale, lease, or licensed to the general public; or will be available in the commercial market place in time to satisfy the delivery requirements of a Government solicitation.

D. Computer Resources: A generic reference to any computer hardware, computer software, or computer peripheral made available to agency staff and used in support of mission activities.

E. Copyright Infringement: The unauthorized use of any original work of authorship that is copyrighted, including computer software.

F. Government Off-the-Shelf (GOTS): A product typically developed by the technical staff of the government agency for which it is created. It is sometimes developed by an external entity, but with funding and specification from the agency. Because agencies can directly control all aspects of GOTS products, these are frequently preferred for Government purposes.

G. DHS Office of the Chief Information Officer (OCIO): The organization that exercises leadership and authority over IT policy and programs DHS-wide.

H. DHS Office of Procurement Operations (OPO): The Department's organization that leads delivery of acquisition services in support of the DHS mission.

I. Host Software List: Approved Server and Infrastructure software, both on the DHS TRM and tested for TSA use.

J. Internal Use Software (IUS): Software purchased from commercial vendors or Government entities off-the-shelf, internally developed, or contractor-developed solely to meet the entity's internal or operational needs. IUS investments are tracked in three phases – Preliminary Design, Software Development, and Post-implementation/Operational. Software development costs are treated as TSA investment property and capitalized in the accounting records if the software development phase costs (including labor) are at least $750,000 and the software application has a useful life of two (2) or more years.

(1) Preliminary Design Phase: Completion of IUS conceptual formulation, design, and testing of possible software project alternatives.

(2) Software Development Phase: Design of the selected IUS alternative, configuration, coding, installation, testing, parallel processing, and acceptance testing; beginning after management authorizes and commits to a software project, believes it is more likely than not that the project will be completed, and has completed the conceptual formulation and design; and ending after final acceptance testing has been successfully completed.

(3) Post-implementation/Operational Phase: Operation and maintenance of IUS, including user training and the conversion of data from the old to the new system.

K. Software License: The permissions, rights, and restrictions imposed on software utilization.

L. Software Management Group (SMG): The SMG is an inter-office group chaired by the Office of Information Technology (OIT) and comprised of IT professionals and key stakeholder groups.

M. Software Program: An organized list of instructions that, when executed, causes the computer to behave in a predetermined manner.

N. System Owner (SO): The Agency official (who must be a Federal government employee) that oversees the procurement, development, integration, modification, or operation and maintenance of an information system in accordance with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37.

O. System Software: A computer program such as the operating system that is used to manage and control a computer hardware and integral components including peripherals.

P. Technical Reference Model (TRM): A framework that categorizes standards and technologies to enable the delivery of service components and capabilities.

Q. TSA-approved Software: System and application software used to satisfy a specific set of user requirements which have been previously tested and approved for use by TSA's Chief Information Officer (CIO) and the SMG. The approved list is maintained by SMG.

R. TSA-owned Software: Any application software or system software purchased by TSA or loaded on TSA-owned or -leased IT equipment such as servers, desktop and laptop computers, and hand-held devices.

S. TSA-unapproved Software: Any software not on the approved software list or any software installed on TSA IT equipment using unauthorized method(s) or service personnel.

T. TSA Enterprise: Composite of all TSA IT resources and facilities.

5. RESPONSIBILITIES:

A. Office of Information Technology (OIT) is responsible for:

(1) Establishing and maintaining TSA's official inventory for software issued and installed on TSA-owned or -leased IT equipment such as servers, desktop and laptop computers, and handheld devices used in support of mission activities; and

(2) Chairing the SMG to facilitate the management, control, and tracking of software.

B. SMG is responsible for:

(1) Maintaining an Approved-client Applications List and Host Software List for the TSA Enterprise;

(2) Providing final authority to ensure that TSA Enterprise software titles on the Approved-client Applications List and Host Software List comply with the TRM;

(3) Maintaining electronic records of all software installations on the TSA Enterprise, including secondary, external installations allowed by certain software license agreements and software licenses;

(4) Establishing TSA software enterprise license agreements, blanket purchase agreements, and task orders;

(5) Establishing software version policies and procedures;

(6) Conducting scheduled and non-scheduled electronic audits of installed software to reconcile against TSA's annual inventory report;

(7) Tracking and controlling all software media, licenses, end-user agreements, certificates of authenticity and related documentation;

(8) Coordinating the review and approval of software development and acquisition requests;

(9) Notifying the TSA Operating Platform Project Manager of approved software purchases or development projects that meet the criteria for capitalization as IUS;

(10) Providing a quarterly inventory of software applications to the TSA Operating Platform Project Manager to facilitate reconciliation with accounting records;

(11) Arranging installations of software on TSA Enterprise assets, including but not limited to cataloging, packaging, delivering, and retrieving;

(12) Updating the DHS TRM for newly approved software, with input from the requesting office or user, in coordination with OIT Business Management Office (BMO), Enterprise Architecture (EA) group;

(13) Tracking all IT peripheral and handheld device software licenses including, but not limited to, personal digital assistants (PDAs);

(14) Providing version controls and upgrades for all applications on the TSA Enterprise; and

(15) Investigating, disabling, and uninstalling unapproved software installed on TSA-owned or -leased IT equipment such as servers, desktop and laptop computers, and handheld devices residing on the TSA Enterprise.

C. Assistant Administrators and equivalents and/or their delegates are responsible for:

(1) Providing proof of ownership of all system and applications software procured, and providing the original media to the SMG;

(2) Providing a test copy of any new application software requested to be added to the Approved-client Applications List;

(3) Identifying requirements for new or expanded software capabilities;

(4) Procuring and funding of additional software and applications;

(5) Ensuring all software and applications procurement are in compliance with DHS MD 0007.1 and applicable TSA policies;

(6) Funding the maintenance agreements for software applications that were procured for specific projects;

(7) Appointing a project representative to coordinate with the TSA Office of Financial Management's Property, Plant and Equipment (PP&E) Accounting Branch for accounting and financial management issues related to IUS; and

(8) Documenting the IUS development project status and costs incurred, and providing timely and accurate information to the PP&E Accounting Branch.

D. SOs are responsible for:

(1) Enforcing internal controls to prevent the unauthorized creation, distribution, or use of software, including measures to verify compliance with these standards, and appropriate disciplinary action for violations of these standards;

(2) Removing unauthorized software from their TSA system boundaries;

(3) Delegating authority for a system to a separate System Manager;

(4) Ensuring that an Information Systems Security Officer (ISSO) is assigned for maintaining the security posture of the system;

(5) Initiating, developing and maintaining the required security documentation (e.g., System Security Plan, Risk Assessment, procurement documentation, and Annual Self Assessment);

(6) Developing and revising procurement request documentation to ensure that the requirements are executable; and

(7) Mitigating identified vulnerabilities.

E. TSA Operating Platform Project Manager is responsible for:

(1) Notifying the PP&E Accounting Branch of approved software purchases or development projects that meet the criteria for capitalization as IUS; and

(2) Providing quarterly, a complete inventory of software applications to the PP&E Accounting Branch to facilitate reconciliation with accounting records.

F. All TSA employees and contractors on the TSA Enterprise are responsible for:

(1) Completing TSA Form 1406, *Desktop Software Request* for approval for installation on the individual's desktop or laptop computer; and

(2) Maintaining and following appropriate policy and procedures concerning handling, control, management, and use of the software installed on government IT resources.

6. POLICY:

A. In accordance with DHS MD 0007.1, no DHS Components, Directorates, or Offices shall enter into or renew software licensing agreements without the approval of the relevant Component, Directorate, or DHS OCIO, pending formulation of the specific policies and guidance associated with this initiative.

B. DHS Components, Directorates, and Offices shall only purchase or renew software licenses that are in compliance with the technology architecture as represented in the DHS Technical Reference Model. Further guidance can be found in the DHS Office of the Chief Information Officer's Office of Applied Technology.

C. DHS Components, Directorates, and Offices shall only use enterprise software licenses agreements for product-specific licenses once enterprise licenses are in place DHS-wide.

D. DHS OCIO and DHS OPO shall negotiate and manage consolidated license enterprise agreements for Department-wide software needs in conjunction with and on behalf of all DHS Components, Directorates, and Offices.

E. DHS OCIO and DHS OPO shall host information workshops to ensure that all DHS Components, Directorates, and Offices ordering officers are clear on the terms of the contract and the ordering procedures for each software license enterprise agreement.

F. DHS OCIO shall provide a listing of targeted software, with projected contract award dates, to allow all DHS Components, Directorates, and Offices an opportunity to develop action plans for renewing or amending existing software contracts.

G. OIT shall ensure that designated SOs oversee the management, control, testing, configuration, and deployment of COTS/GOTS applications, server and custom software on all systems within their TSA system boundaries.

H. OIT shall ensure that approved commercial software is appropriately licensed and maintained for the environment and sufficient to meet user demand.

I. TSA employees shall not use Government funding to acquire, create, operate, or maintain computer software in violation of applicable copyright laws. If a TSA employee or contractor becomes aware of a proposed misuse of funds, the TSA employee is required to contact their immediate supervisor and the contractor should notify the contracting officer technical representative (COTR) or other

appropriate Government Official to ensure that the purchase receives an appropriate legal review prior to award.

J. TSA employees and contractors shall use software only in accordance with the specific license agreement. Unless otherwise provided in the license, any duplication of copyrighted software, except for backup and archival purposes, is a violation of the Copyright Act and contrary to TSA's standards of conduct.

K. The use of unauthorized or unlicensed software and personally-owned software and the unauthorized installation of any software are prohibited.

L. The Assistant Administrators and equivalents and/or their delegates will require the contractor to identify software and licensing cost in contracts separate from hardware purchases, maintenance agreements and warranties.

M. TSA SOs shall enforce internal controls to prevent the unauthorized creation, distribution, or use of software, including measures to verify compliance with these standards, and appropriate disciplinary action for violations of these standards. Unauthorized software may be removed promptly by TSA SOs without prior notice to the employee or contractor.

N. Copyright violators are subject to civil damages up to $100,000, and criminal penalties, including fines and imprisonment. Any employee or contractor that copies, acquires, or uses unauthorized copies of computer software shall be disciplined as appropriate under the circumstances. Such discipline may include termination for intentional or repeated violations. TSA does not condone the illegal duplication of software.

NOTE: The use of software without a valid license could constitute infringement of the owner's exclusive rights under copyright or, occasionally, patent law, allowing the owner to sue the infringer.

O. All software requirements shall be reviewed by a SMG representative prior to submission to requesting office's Assistant Administrator or equivalent for approval.

P. All software requirements shall go through the TSAITBuy process.

Q. Only authorized IT Specialists, with prior SMG approval, shall install or uninstall software on the TSA Enterprise.

7. PROCEDURES:

A. In accordance with licensing agreements, all TSA employees and contractors requiring software applications that are not part of the approved desktop or mobile device image shall complete and submit TSA Form 1406, *Desktop Software Request*.

B. TSA staff and contractors shall submit all original software media and licenses for tracking purposes to their SMG representative. For a current listing of SMG representatives, visit the SMG Website.

C. TSA Supervisors, IT points-of-contact (POCs), or COTRs send an email to Exit-TSA@dhs.gov with the name, email address, phone number, organization/branch, office number, and date of departure of all exiting employees and contractors so that software licenses can be recouped.

NOTE: Office of Law Enforcement/Federal Air Marshal Service (OLE/FAMS) personnel, contact the OLE/FAMS helpdesk to comply with this procedure.

8. **APPROVAL AND EFFECTIVE DATE:** This policy is approved and effective the date of signature unless otherwise specified.

APPROVAL

Signed October 5, 2011

_____ _____
Dr. Emma Garrison-Alexander Date
Assistant Administrator for Information Technology/
Chief Information Officer

EFFECTIVE

_____
Date

Distribution: All TSA employees and contract personnel
Point of Contact: OIT, Software Management Group, Applications@dhs.gov